МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

МАГОМЕДОВ ГАДЖИМУРАД АБУБАКАРОВИЧ

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ В ЭЛЕКТРОННЫХ (КОМПЬЮТЕРНЫХ) СЕТЯХ

Направление подготовки 40.03.01 – «Юриспруденция»
юридического факультета СГУ им. Н.Г.Чернышевского

Автореферат бакалаврской работы

Научный руководитель
доцент, к.ю.н, доцент кафедры уголовного,
экологического права и криминологии О.Р. Шайхисламова

Заведующий кафедрой уголовного,
экологического права и криминологии
канд. юрид. наук, доцент Е.О. Глухова

Саратов 2024

Введение

Актуальность темы выпускной квалификационной работы заключается в том, что охрана компьютерной информации должна обеспечиваться как часть приоритетной области социального порядка. Стремительное становление компьютерных спецтехнологий и глобальное распространение электронных компьютерных систем фактически во всех сферах жизни человека затронуло множество аспектов в области правового регулирования отношений, связанных с компьютеризацией социума. Данное обстоятельство поднимает вопрос об образовании индустрии компьютерного права, одним из основных аспектов которой является так называемая компьютерная узурпация.

Также об актуальности темы исследования свидетельствует разнообразие допустимых способов совершения киберпреступлений и их количество. По данным МВД, каждое третье преступление в 2023 году было совершено с использованием цифровых инструментов. Объектами посягательства в данных преступлениях могут быть сами технические средства (компьютеры и периферийные устройства) в виде физических объектов, программного обеспечения, баз данных и информации как таковой. Да и сами преступления с применением компьютерных спецтехнологий исключительно многообразны и трудны. Объективная сторона таких преступлений может включать, скажем, перехват конфиденциальных сигналов от пейджинговых и сотовых устройств, подделку кредитных карт, несанкционированный доступ к информации, внедрение программных логических бомб, влияющих на компьютерную систему, становление и распространение вирусов, кражу информации с компьютерного носителя.

В России научное сообщество не занималось компьютерной преступностью до начала 1990-х годов, да и в настоящее время степень научной проработанности данной темы в отечественной литературе достаточно низка. В последние годы был опубликован ряд работ, в основном касающихся криминологических и криминалистических аспектов

компьютерных правонарушений. Рассмотрение киберпреступности именно в уголовно-правовом аспекте, на наш взгляд, сегодня значительно меньше отражено в научной литературе. Монографии и статьи в основном относятся к предмету, а также инструментам, используемым для несанкционированного действия компьютера, и их связи друг с другом. Некоторые работы содержат конструктивную критику главы 28 Уголовного кодекса Российской Федерации[1] (далее УК РФ) как с уголовно-правовой, так и с информативной точки зрения.

Не только теоретически, но и фактически в нашей стране не было резкой реакции на волну компьютерной преступности. Криминальный мир неизменно был на шаг впереди правоохранительной системы, охватывая лучшее, что может предложить социум. Но, невзирая на доступные источники и способы, борьба с киберпреступностью по-прежнему весьма ограничена. Законодательные органы, можно сказать постоянно подстраиваются под изменения данного вида преступности, принимая соответствующие юридические меры для противодействия этому новому виду правонарушений.

Объектом исследования выступают преступления в сфере компьютерной информации, а также общественные отношения, связанные с их совершением.

Предметом исследования является уголовное законодательство, устанавливающее ответственность за совершение преступлений в сфере компьютерной информации.

Цель исследования состоит в изучении понятий и видов преступлений в сфере компьютерной информации с акцентированием на достоинствах и недостатках их законодательной регламентации, и анализом правил квалификации указанных преступлений.

Исходя из поставленной цели **задачами** исследования являются:

[1] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 г. № 63-ФЗ (ред. от 06.04.2024 г.) // СЗ РФ. 1996. № 25. Ст. 2954; 2024. № 15. Ст. 1972 .

1) рассмотрение становления и развития законодательства Российской Федерации о компьютерных преступлениях;

2) определение понятия и видов преступлений в сфере компьютерной информации;

3) исследование неправомерного доступа к компьютерной информации;

4) анализ создания, использования и распространения вредоносных компьютерных программ;

5) изучение нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Степень научной разработанности темы исследования. В последние годы вопросы преступности в области компьютерной информации все чаще начали освящаться в научной литературе. Исследованием указанных вопросов занимались: Вехов В.Б., Дворецкий М.Ю., Евдокимов К.Н., Ефремова М.А., Казарин О.В., Карабанова О.В., Лебедев В.М., Летелкин Н.В., Малыковцев М.М., Маслакова Е.А, Ролик А.И., Саркисян А.Ж., Чупрова А.Ю. и другие. Однако, невзирая на теоретическую и практическую значимость указанных исследований, в них не уделено достаточного внимания анализу проблем, которые связаны с преступлениями в сфере высоких информационных технологий.

Нормативно-правовой основой исследования являются: Конституция Российской Федерации[2], Уголовный кодекс Российской Федерации, Федеральный закон «Об информации, информатизации и защите информации»[3], Федеральный закон «О связи»[4], Федеральный закон «Об

---

[2] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г.) (ред. 14.03.2020 г.) // Российская газета. 1993. 25 дек.; Собрание законодательства РФ. 2020. № 11. Ст. 1416.

[3] Об информации, информатизации и защите информации: Федеральный закон от 20.02.1995 г. № 24-ФЗ (утратил силу: ФЗ РФ от 27.07.2006 г. № 149-ФЗ) // СЗ РФ. 1995. № 8. Ст. 609; 2006. № 31 (часть I). Ст. 3448.

[4] О связи: Федеральный закон от 07.07.2003 г. № 126-ФЗ (ред. от 06.04 20224 г.) // СЗ РФ. 2003. № 28. Ст. 2895; 2024. № 15. Ст. 1960.

участии в международном информационном обмене»[5], и некоторые другие нормативно-правовые акты. При этом следует отметить, что нормативные акты, утратившие силу, также имеют значение при исследовании данной темы.

Методы исследования, использованные при написании работы: общетеоретический, анализ, синтез, логический, сравнительно-правовой, исторический, статистический, а также метод анализа и толкования правовых актов.

Структура выпускной квалификационной работы состоит из введения, двух глав, объединяющих пять параграфов, заключения и списка использованной литературы.

Основное содержание работы

В главе первой рассматривается общая характеристика преступлений в сфере компьютерной информации. Глава состоит из двух параграфов.

В первом параграфе изучается становление и развитие законодательства Российской Федерации о компьютерных преступлениях.

Во втором параграфе определяются понятие и виды преступлений в сфере компьютерной информации.

Глава вторая исследует уголовно-правовую характеристику преступлений в сфере компьютерной информации. Данная глава состоит из трех параграфов.

Первый параграф раскрывает неправомерный доступ к компьютерной информации.

Второй параграф изучает создание, использование и распространение вредоносных компьютерных программ.

---

[5] Об участии в международном информационном обмене: Федеральный закон от 04.07. 1996 г. № 85-ФЗ (утратил силу: ФЗ РФ от 27.07.2006 г. № 149-ФЗ) // СЗ РФ. 1996. № 28. Ст. 3347; 2006. № 31 (часть I). Ст. 3448.

Третий параграф исследует нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Заключение

В заключение выпускной квалификационной работы можно сделать следующие выводы:

1. В связи с активным ростом киберпреступности и кардинальными изменениями в средствах и способах совершения многих преступлений, связанных прежде всего с компьютерными технологиями, информационными ресурсами, информационно-телекоммуникационными системами, необходимо решить проблемы применения статей, предусматривающих уголовную ответственность за преступления в сфере компьютерной информации. Как показывает практика, преступления в сфере компьютерной информации в основном являются способами совершения других преступлений, посягающих на собственность, общественную безопасность, здоровье населения и т.д.

2. Преступность, как и другие социальные явления, все больше и больше переходит в киберпространство, что существенно усложняет процесс раскрытия такого рода преступлений. Многие преступления совершаются не выходя из дома с использованием различного рода технических средств, позволяющих проникать в средства хранения, передачи, обработки компьютерной информации. Для эффективной борьбы с киберпреступлениями необходимо совершенствовать систему применения норм уголовного законодательства и разработать единые подходы к правилам квалификации этого вида преступлений.

3. Самыми часто совершаемыми преступлениями в данной сфере являются преступления, подразумевающие неправомерный доступ к компьютерной информации. Они составляют более половины всех преступлений, ответственность за которые предусмотрена главой 28 УК РФ.

Этому способствует, озвученное выше непрерывное и стремительное развитие компьютерных технологий и широкое использование электронно-вычислительных систем практически во всех сферах человеческой жизнедеятельности.

4. Исследование различных определений киберпреступности позволили сделать вывод о том, что многие авторы наряду с термином «киберпреступность» используют термины «компьютерные преступления» и «преступления в сфере компьютерной информации» как синонимы, в связи с чем возникает вопрос о соотношении данных понятий. Полагаем, что термин «киберпреступность» шире понятия «компьютерные преступления», так как последний термин указывает на совершение преступлений с помощью или против компьютеров и компьютерных систем, тогда как понятие «киберпреступность» включает все возможные варианты совершения преступлений в компьютерной среде, в сфере высоких технологий, а также преступления, направленные против различных систем и каналов связи, включая глобальную сеть Интернет, либо совершенные с их помощью.

Говоря о перспективе совершенствования ст. 272 УК РФ, следует подумать и о введении дополнительных квалифицирующих признаков, таких как совершение неправомерного доступа к компьютерной информации по мотивам политической, религиозной, расовой и иной форм ненависти. Возникают споры относительно необходимости законодательного закрепления в УК РФ пояснения сущности общественно опасных последствий. Безусловно, постановления Пленума Верховного Суда РФ играют важную роль в правовой системе РФ. Однако согласно закону, постановления были и остаются актами толкования права, имеющими рекомендательный характер и необязательны к исполнению.

Учитывая вышеизложенное, предлагается изложить текст ст. 272 УК РФ в следующей редакции:

«Статья 272. Неправомерный доступ к компьютерной информации:

1. Совершение неправомерного доступа к охраняемой законом компьютерной информации и последующее ознакомление с ней наказывается ...

2. То же деяние:

а) повлекшее за собой уничтожение, повреждение, блокирование, модификацию либо копирование информации - наказывается …;

б) причинившее крупный ущерб или совершенное из корыстной заинтересованности - наказывается …;

в) совершенное по мотивам политической, религиозной, расовой и иной форм ненависти - наказывается …;

г) совершенное путем обмана или злоупотребления доверием потерпевшего - наказывается …;

д) совершенное с целью сокрытия другого преступления - наказывается ...

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, - наказываются ...

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или угрозу их наступления, - наказываются ...»

Существенным упущением является отсутствие уголовной ответственности за покупку, приобретение или получение вредоносных компьютерных программ. Общественная опасность такой программы, заведомо предназначенной для совершения неправомерных действий, на сегодняшний день очевидна. Поэтому лицо, приобретающее ее, следует подозревать в подготовке к совершению преступления, предусмотренного в ст. 273 УК РФ, так как другого прямого назначения у указанных программ нет.

Учитывая, что Уголовный кодекс РФ является, по сути, единственным источником уголовного права, что видно из содержания ст. 1 УК РФ, следует

законодательно закрепить понятие вредоносной компьютерной программы в целях совершенствования процесса квалификации и расследования преступления. На основе анализа различных подходов к толкованию вредоносной компьютерной программы предложим авторское определение – программа, созданная на языке программирования и заведомо предназначенная для неправомерного доступа к компьютерным устройствам и воздействия на них в целях уничтожения, повреждения, модификации, копирования компьютерной информации, ознакомления с ней, слежения за компьютерным устройством, ограничения доступа к информационно-телекоммуникационным ресурсам в сети Интернет, нейтрализации средств защиты компьютерной информации.

С учетом результатов анализа предлагаем следующие изменения в действующую редакцию ст. 273 УК РФ «Создание, использование, распространение и приобретение вредоносной компьютерной программы и иной компьютерной информации.

1. Создание, использование, распространение и приобретение вредоносной компьютерной программы и иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, повреждения, блокирования, модификации, копирования компьютерной информации, а равно и ознакомления с ней, слежения за компьютерным устройством, ограничения доступа к информационно-телекоммуникационным ресурсам в сети Интернет, нейтрализации средств защиты компьютерной информации, – наказываются …

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору, организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, – наказываются …

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, – наказываются …»

Таким образом, преступлениями в сфере компьютерной информации являются предусмотренные уголовным законом общественно опасные деяния, причиняющие вред или создающие опасность причинения вреда безопасности производства, хранения, использования либо распространения информации или информационных ресурсов. К указанным преступлениям относятся: неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.